**Whitepaper Draft**

**Introduction**

The aim of this paper is to explain an issue surrounding law and government related processes, and suggests a solution in the form of a replacement system to manage said processes, using a decentralized, hash-based chain of informational blocks, also known as a ***blockchain.***

The challenges facing this solution will be explained in depth, as well as the benefits.

**Table of Contents**

1. **In-depth explanation of the Issue**
2. **In-depth explanation of the Solution**

**- GovCoin**

1. **Implementing the Solution**

**1. In-depth explanation of the issue**

Governments, in general, always struggle to adapt to newer technologies due to the massive scale of changes that need to take place. This leaves individuals who have to use their government’s services wasting their time in an ever-evolving world, where millions upon millions of pieces of information are sent and handled ***per second, in the Digital World.***

As an example, let’s say you need to get a passport.

You have to ***physically***go to some government building, carrying ***all the necessary information***, ***wait in line,*** and ***verbally exchange*** pieces of information with an ***employee*** which will then ***upload your request*** to the system.

After all of that, you would receive your passport in a week or two, depending on how loaded / backlogged ***the system*** is.

This raises a few questions:

Why did you have to go the government building in the first place?

Why Wait in line?

Why exchange information ***verbally*** with an error-prone human?

Why not communicate with ***the system*** directly?

And, most importantly, why wait for a whole week (or more) after all of that?

A potential solution to this issue is to transfer – at least a portion – of the government’s services to a digital solution i.e. An online website, with a user-friendly UI, where individuals may use certain services without having to waste as much time in a physical world.

Initially, this might seem good on-paper, but in the real world, a few issues arise.

Because, while such a system might be able to function well enough ***most*** of the time, a centralized backend would most definitely **not** be able to handle a sudden inflow of users who all aim to do the same thing.

For example, during the holiday season, many people decide to renew their passports, all at once.

Additionally, a system of such scale would have countless security flaws which make it susceptible to hacking attacks.

And as a country grows in population and expands its services, the backend systems will have to grow as well, amplifying the effect of current issues.

The mentioned flaws in such a system deprive it of most of its valuable aspects, as compared to the current situation.

The solution suggested in this paper provides a system that covers all mentioned flaws, with less expenses, higher security, and easier maintainability.

**2. in-depth explanation of the solution**

The proposed system is a decentralized, reward-based system that implements the use of ***legal contracts,*** similar to ***smart contracts*** in the ***Ethereum Blockchain.***

A **Legal Contract** can be considered a sub-type of a smart contract, with the difference that only official recognized parties may make a **legal contract.** This means that at any given time, a user can be confident that they are filling out an official contract, offered strictly by official parties i.e. The Government.

The system will be built on its own blockchain, which will be optimized for relevant services.

It will also implement the use of ***GovCoin***: a specially created cryptocurrency which will be used to reward ***active processing nodes*,** or pay for given services, as well as other purposes mentioned in a later section.

An ***Active Processing Node (APN)*** is any active device on the blockchain, contributing processing power to increase speed, efficiency, and security of the blockchain, as well as ***mining*** for new blocks.

The previously mentioned digital solution depends on a government supported, Centralized Backend Server to handle and process user requests.

In the proposed system, however, any user can choose to become an ***APN,*** where said user can offer their device(s) to increase the processing power of the system, or mine new blocks, and be rewarded in proportion with their work.

As a side note. A user who is an **APN** does not give up the use of their device completely, nor even partially. The process will be designed in a way that makes it least intrusive and power-consuming to the **APN**, which will encourage more users to become **APNs** themselves.

Hence, the issue of scalability is solved, because as population and demand increases, the number of ***active processing nodes*** will also automatically increase.

**-** **An Example**

In contrast to the example given in the previous section, let’s say you needed to get a passport using this new system.

You open up your smartphone, open the relevant app or webpage, find the correct service for your needs, check a few boxes to complete your ***legal contract****,* and pay a certain amount of **GovCoin** as processing fee that varies depending on how quickly you want your request to be processed.

A few moments later, your passport has been created and you can expect to receive it as soon as the physical copy has been made. All of this you could do from anywhere in the world.

An automated **legal contract** has taken care of everything that an employee would have had to manually ask of the user, and then enter into the system, potentially making a mistake somewhere along the way.

This has the potential to save days’ worth of time ***per individual.***

Since all given information is stored digitally, the risk of misinterpretation is minimal.

There is no “standing in line”, and no waiting for potentially weeks while the system clears up its backlog. And no chance to ***Bribe*** someone to overlook some details.

**- Risks**

Such a system, secure and reliable as it is, has a few risks, such as the ***51% attack,*** in which a group of miners who control more than 50% of the network’s mining rate could interrupt the recording of new blocks, and record new blocks with compromised information.

The risk of such an attack is more noticeable on smaller-scale blockchains. On a government-scale where an entire population is taken into account, there is very minimal risk of a group of attackers gaining the needed computing power.

**- GovCoin**

What is GovCoin? Why is there need for such a cryptocurrency?

GovCoin is the official cryptocurrency used throughout the network.

Its purposes include (but are not limited to) the following:

Any government related payment, such as Taxes.

Exchanging cryptocurrency for digital / non-digital currency

Paying the fee for using a government service.

Paying an extra fee for said service depending on speed preference.

GovCoin will be generated as a compensation for users contributing to the network as **APNs.**

**3. Implementing the solution:**

Governments around the world always struggle to keep up with what technology has to offer simply because of their massive scale.

The entire infrastructure of a government willing to implement this solution will need to change completely, which is a very time-consuming task capable of generating many errors and vulnerabilities.

The proposed solution takes into account *how* a given government entity will transition into a completely new system in a digital environment.

The official announcement of the government’s transition to the system can only happen once there are enough users to make the system self-sufficient.

**4. Conclusion**

Governments have outdated methods that rely on outdated technology, being performed by error-prone, and more importantly corruptible humans, and usually relying on a centralized management system.